Application of Fault Containment Principles to EMC

Reinaldo "Ray" Perez
Jet Propulsion Laboratory
California Institute of Technology
4800 Oak Grove Drive, Pasadena, CO 91109
reinaldo.j.perez@jpl.nasa.gov

***Abstract*--A hardware fault in aerospace is an undesired response to a designed engineering function in hardware. Therefore, in aerospace systems fault management is of prime importance. An important aspect of hardware faults is fault propagation. Fault propagation (also known as failure propagation) is a condition where a fault will not only produce an undesired hardware response, at its location of origin, but the fault will also propagate to other interfaced hardware and cause additional faults, or failures. Fault containment is necessary to avoid fault propagation. A *fault containment region* is an electronic or electromechanical region within a given hardware assembly where a fault in that region will not physically propagate to other regions of the assembly, and beyond. Rather, the fault will cause a functional failure of the hardware, where the fault occurred, without causing any additional propagated failures. Electromagnetic Compatibility (EMC) is a desired state in aerospace hardware. Electromagnetic Interference (EMI) in aerospace hardware is a fault condition of EMC. Like other faults EMI can also propagate to other aerospace hardware unless it occurs inside an *EMI containment region*. The paper addresses the concepts of fault containment region and introduces the concept of *EMI containment region* with examples of both.**

TABLE OF CONTENTS

1. INTRODUCTION

A lack of EMC in a hardware assembly due to one or more EMI anomalies can cause an abnormal functional response in an assembly. Therefore, depending on the severity of the EMC problem a potential for an EMI-induced hardware anomaly is possible. Likewise, depending on the nature of the EMC problem the EMI-induced hardware anomaly can have the capability of propagating to other assemblies it interfaces. Therefore, we can define a new concept known as an *EMI fault containment region* (EMI FCR) in an assembly as an electronic or electromechanical region within a given assembly where an EMI-induced anomaly in that region will not propagate to other assemblies. Rather, the EMI-induced anomaly will only cause a localized functional anomaly (or a fault) of the hardware where the anomaly occurred.

It is often difficult to consider that a lack of EMC could eventually cause an anomaly or a fault capable of propagating within an aerospace system, but such scenario has been observed and was briefly discussed in [7] with its un-conventional solution (scenario presented itself in flight). The scenario is not common. EMC problems are most often localized. Standard EMC tests are designed to discover local EMC problems. Most solutions to EMC problems are also localized. This is generally a good assumption but such rationalization ignores a few potential issues concerning the nature of EMC problems: (a) EMC problems can arise due to the lack of signal/power compatibility between two or more assemblies, interfaced with each other, and within a system, (b) there are new signatures of EMI emissions (conducted and/or radiated) due to the combined effects of emissions from a several assemblies in a system, and (c) there can be exposure to new EMI susceptibilities problems in a system due to the combined effects of EMI sources in a system. Therefore, EMI-induced anomaly propagation (or EMI FCR) within a system is quite possible because the EMI FCR has now been unintendingly expanded, and in worst cases, it can include the whole system. The un-intended expansions of EMI FCRs are particularly of concern in the areas of conducted and radiated susceptibility.

Before we address in more details the concept of EMI FCRs, we must first address more detailed knowledge about fault containment regions in general.

2. FAULT CONTAINMENT REGIONS

The concept of fault containment regions (FCRs) is not new [1]. The concept of FCRs has been used in computer-based fault tolerant systems [2]. It has also been used quite extensively in computer networks [3]. We introduce the FCR concept as a tool for the simplification of the process of EMI containment which is the main salient feature of this paper. The concept of FCR is basically illustrated in Fig. 1. As shown in Fig. 1, a well-defined FCR does not allow any failures within the FCR to propagate outside the protected region.

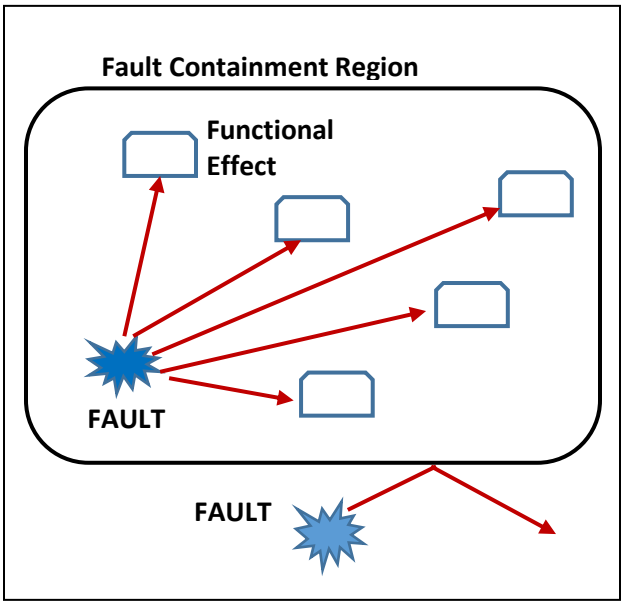

Figure 1. Basic concept of FCR

The failures stay inside the FCR. Likewise, the FCR does not allow any failure outside the FCR to propagate into the protected region. In essence the FCR does not allow failure propagation as shown in Fig 2 where an assembly with four identified FCR (FCR 1 through FCR 4) does not allow failure propagation among the four FCRs.

For this paper, a FCR is defined as an electronic or electromechanical region within an assembly where a failure in that region will not physically propagate to other electronic or electromechanical regions in the hardware assembly or beyond the assembly, and likewise will not allow external electrical or electromechanical failures to affect the FCR. Therefore, in principle a failure in the electronic or electromechanical FCR can only cause a functional failure of the corresponding hardware assembly without such functional failure causing any additional propagated functional failures in other electronic or electromechanical regions of the hardware assembly and beyond.

By definition there is no failure propagation in FCRs. However, failure propagation could occur in a FCR if: (a) the FCR has not been well defined and it actually extends into the boundaries of other FCRs (and possibly other hardware), and (b) failures occur at the physical hardware interfaces that join the FCRs.

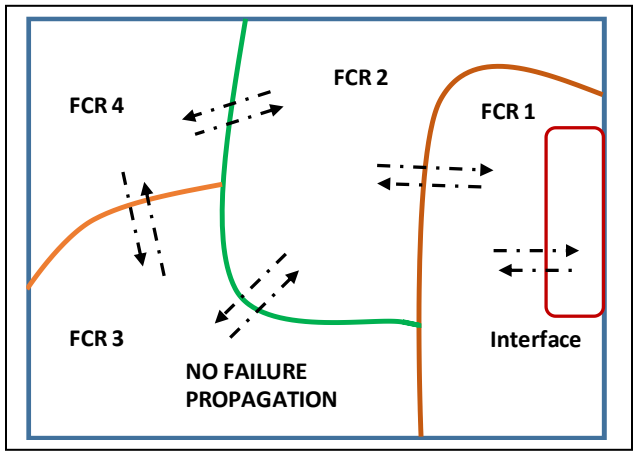

Figure. 2. FCR not allowing failure propagation

A simple example of the former is the very recent issue with the crashes of two Boeing 737 Max 8 in which errors produced by a single angle of attack (AoA) sensor (two sensors were available, but only one was being used) due to its failure (attributed to potential physical damage or internal fault) caused aircraft attitude errors to propagate (i.e. failure propagation) to the maneuvering characteristic augmentation system (MCAS) of the aircraft. The MCAS fight management software was not able to address the fault propagation in an effective manner. In essence both the AoA and MCAS were in the same FCR, and such understanding may not have been realized in the aircraft design process. Secondly, and as stated, failures at the physical hardware interfaces that joints FCRs can also cause failure propagation across FCRs. These failures are much more common. An electrical or electromechanical failure at the interfaces between FCRs can allow: (a) a failure at the interface itself to propagate to either one (or both) FCRs, and (b) allow errors (e.g. signal degradation/distortion) to propagate from one FCR to another (i.e. the interface failure itself introduces errors in the FCRs for the FCRs that are physically connected).

It is important to well define the size of the FCRs because the size of a FCR can vary, depending on the nature of the piece parts components failure modes, the type of components involved, the design of the hardware, and even the failure history of the parts or components used in the hardware. Defining the size or extent of the FCR is arrived to by the reliability engineer through several means:

hardware drawings and schematics, parts lists, hardware functional descriptions, knowledge of all signal names, knowledge of all signal interfaces, knowledge of all signals functions, and the development of the circuit data sheets (CDS).

3. General Faults And FCRs

The relevance of this section is discussed in Section 7. When addressing fault propagation, one of the most common reliability analyses performed is the Interface Failure Modes Effects and Criticality Analysis (IF FMECA) [4-6]. The primary goal of the IF FMECA is to identify and analyze potential failure modes at the electrical and electromechanical interfaces of assemblies in order to eliminate or minimize the effects of the failure modes that are most disabling. The IF FMECA identifies failure modes that can propagate from one FCR to another via failures at the interfaces connecting the FCRs. For electronic and electromechanical assemblies, the piece-part IF FMECA is the most detailed IF FMECA. The piece-part IF FMECA identifies failure modes of electrical and electro-mechanical components or parts, on both sides of the FCRs, and assess if the failure modes of these components can propagate across the interfaces. In order to perform the IF FMECA in a productive manner the concept of FCRs must first be used. This means that we start with defining the FCRs and then perform the IF FMECA based on the results of the FCRs analysis.

4. The Concept Of EMI FCRs

As previously stated EMI is most often a localized problem in hardware. An aerospace hardware with EMI issues will not function properly. For example, if the hardware is susceptible to radiated electromagnetic emissions, most likely it is due to its highly sensitive analog electronics (e.g. as in sensors, transducers), or the hardware itself is a radio frequency transceiver, or the hardware has become an unintentional receiver. If the hardware is susceptible to conducted electromagnetic emissions, most likely the hardware is sensitive to differential and/or common mode noise flowing through its different conductive paths (e.g. cabling, wires, connectors pins, vias, ground planes, and others—including parasitics!). The overall outcome to EMI susceptibility by a hardware is degraded electrical performance, which often translates into the degraded data transmitted by the hardware. Though degraded data can be transmitted to other hardware, causing errors, the EMI itself stays most often localized to the hardware where it originated, and because most often the EMI problem is localized, EMC testing of the hardware is also localized. Fig. 3 shows a composite setup of the four major EMC tests performed on a typical individual hardware, also known as the equipment under test (EUT).

An EMI FCR is defined as the region within a hardware beyond which EMI will not propagate. There is no EMI coming in or going out to/from the EMI FCR. Though EMI in the hardware can cause a degraded performance in the hardware itself, and potential errors transmitted to other hardware (e.g. to hardware connected by an interface), EMI will not propagate beyond the EMI FCR.

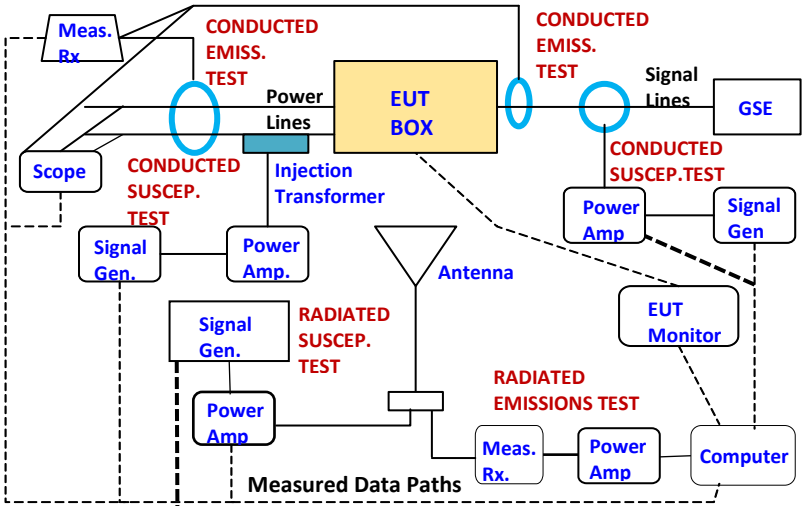

Figure 3. Typical setup for EMC Testing

The basic concept of EMI FCR is shown in Fig. 4. The figure shows hardware (HWR) #1 connected to HWR # 2 via an interface (data, signals interface). HWR #1 contains a source of EMI (radiated, conducted, or both). If HWR #1 is well designed to contain its own sources of EMI, no EMI noise will propagate through the functional and interface boundaries of HWR #1. It is then said that HWR #1 has a FCR that bounds its functional and interface limits. If HWR #1 is not well designed to contain its own sources of EMI, then EMI noise starts propagating outside its own functional and interface boundaries, as illustrated in the figure. This is illustrated by showing an expanding EMI FCR. The EMI FCR could eventually reach up to HWR #2's functionals and interface boundaries; and it is at this point where EMI failure propagation has occurred.

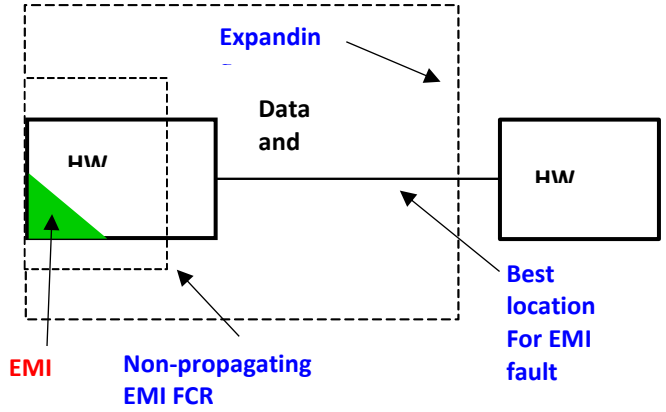

Figure 4. Conceptual EMI FCR.

There are two scenarios for EMI propagation across an EMI FCR: (1) a deficient EMC design at an interface crossing the EMI FCR boundary and/or (2) an erroneous estimation of the extent of the EMI FCR. For the former scenario (i.e. scenario (1)), consider Fig. 5 where HWR #1 contains a known source of EMI as discovered via EMC testing. The figure shows that a good EMC design will not allow EMI to propagate beyond the FCR of HWR #1, a poor design will extend the EMI FCR to HWR #2. EMI will propagate to HWR #2 due to a deficient EMC design in the FCR boundary between HWR #1 and HWR #2. A much poorer design will extend the EMI FCR to HW #3 and the EMI will propagate to HW #3 due to a deficient EMC design in the FCR boundary between HWR #2 and HWR #3.

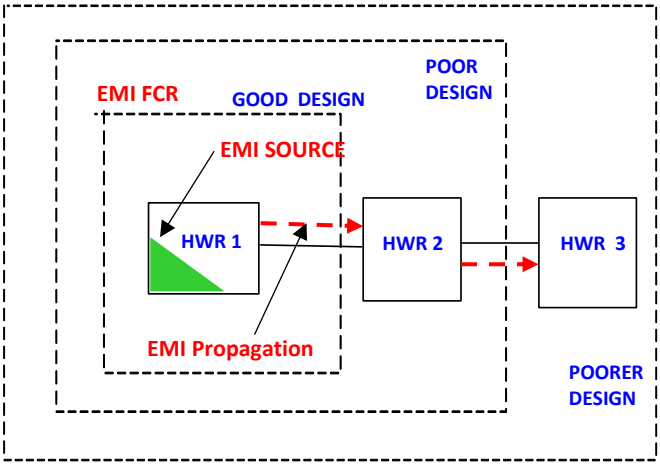

Figure 5. EMI Propagation vs Fault Containment

For the latter scenario (i.e. scenario (2)) consider Fig 6. In the figure there are two sources of EMI, in HWR # 1 and HWR #3. The EMI FCR for HWR #1 is characteristic of a good design, but the EMI FCR for HWR #3 is so extensive that it overlaps the EMI FCR for HWR #1. Therefore, EMI will propagate from HWR #3 to HWR #1 as shown.

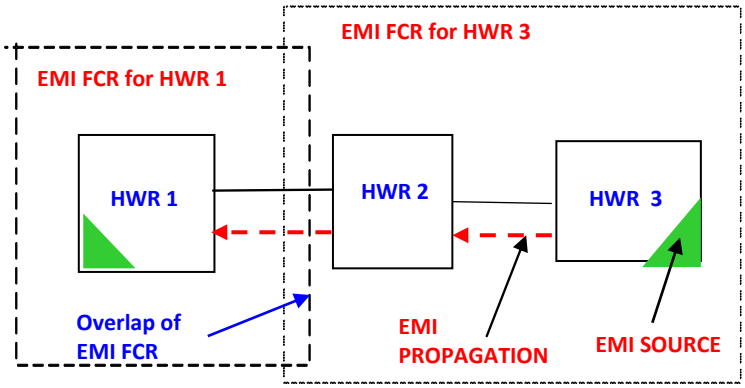

Figure 6. FCRs overlap in Poor Designs.

The overlap is possible for two reasons: (a) HWR #3 cannot prevent its own EMI from exiting via its interface, and (b) HWR #2 does not have the capability of stopping EMI propagation, regardless of where it comes from, even if does not itself contains a source of EMI. Let's consider again the previous example of the Boeing 737 Max 8 accidents. If you assume that a large EMI event, such as a cloud-to-cloud lightning strike, could have occurred near the vicinity of the only available aircraft's AoA sensor (the aircraft has two AoA sensors but only one was being used, as previously stated), represented herein by HWR #3, and if such an EMI event could have stressed the AoA's analog sensor electronics (represented by HWR #2), causing it to malfunction, and noticing that HWR #2 does not have an EMI FCR, it is easy then to understand from Fig. 5 how the malfunction of HWR #2 could also propagate to HWR #1.

5. FCRs In EMI Propagation Solutions

In this section we transition from the conceptual understanding of EMI FCR to an actual application on the usage of EMI FCR to eliminate or diminish EMI propagation. As an illustrative example of this effort we consider Fig.7 which shows a data processing system within an aerospace hardware for acquiring and processing science data.

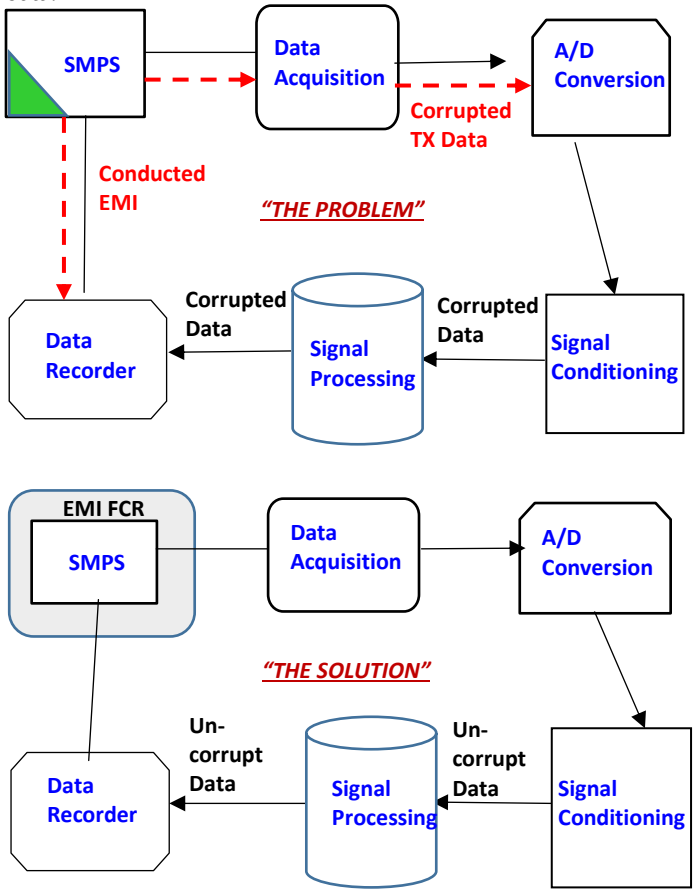

Figure 7. Example EMI FCR Solutions

Notice that Fig. 7 is a "system". The data processing system depicted is only partial for the purpose of this illustration. The data processing system contains a switching mode power supply (SMPS) which provides DC power to a data acquisition unit (i.e. acquires analog sensor data), and also

provides power to a data recording storage unit (stores digital information of science data). The other hardware in Fig. 7 get their power from elsewhere. Other hardware components in the figure are the A/D converter unit which converts the acquired analog data into digital data, the signal conditioning unit which conditions the digital data before being processed, and the signal processing unit which converts the digital data to useful data streams and process the data streams into information.

The top half of Fig. 7, titled "The Problem" shows that the SMPS is a source of conducted EMI which manifest itself in conducted EMI emissions as shown in the top half of Fig. 7. Even though the SMPS may have satisfactorily complied with the requirements of power line conducted emissions tests, as measured in Fig. 3, the required tests are performed to measure the magnitude and frequency profile of the power line conducted emissions, and compare the measured results with standard requirements. However, for the hardware set up in Fig 7, true compliance of the SMPS to power line conducted emissions is dependent on the levels of susceptibility of the connected hardware (i.e. the data acquisition and the data recorder) to the existing levels of conducted emissions emanating from the SMPS. The top half of Fig. 7 shows that conducted EMI affects the performance of the data acquisition and data recorder units and the end results is corrupted data being stored, as shown in the figure. It is also important to notice that there are not EMI FCRs protecting any of the hardware, which means there has not been a design effort to contain EMI within the hardware. In this example the lack of FCRs allows conducted EMI to propagate. The bottom half of Fig. 7, titled "The Solution" shows the remedy to eliminate EMI failure propagation and its consequential results of generating corrupted data. The solution is quite simple; allow an EMI FCR to protect the SMPS. This means that the interface between the SMPS and the data recorder unit, and between the SMPS and the data acquisition unit must be designed such that the conducted emissions from the SMPS are below both, the susceptibility levels of the data recorder and data acquisition hardware. It can therefore, be concluded that the strategic identification and subsequent implementation of EMI FCR can significantly reduce the propagation of EMI noise in aerospace hardware.

6 System Solutions To EMI Propagation

In the previous section it was discussed how the strategic placement of hardware with well-designed EMI FCRs can eliminate EMI propagation. This approach becomes even more advantageous when addressing EMI propagation within an aerospace system or among aerospace systems, and an illustration of the strategic advantage of EMI FCRs placement can be shown in Fig. 8. The figure shows two systems (system 1 and system 2). The two systems communicate with each other via connected interfaces, as shown. Each system contains its own suite of hardware. System 1 contains six hardware assemblies. System 2 contains five hardware assemblies. Within a system, the hardware that was designed with an EMI FCR is named by its FCR number (e.g. FCR #4 in system 1 refers to HWR # 4 having a FCR). The hardware that was designed without a FCR is named by its hardware number (e.g. HWR #1 in system 1 does not contains a FCR). The same approach is used for System 2. As can be shown in Fig. 8, System 1 contains six hardware assemblies of which only three have EMI FCRs. System 2 contains five hardware assemblies of which four have EMI FCRs. Fig. 8 also shows the hard-wired interfaces joining the hardware assemblies within System 1 and within System 2.

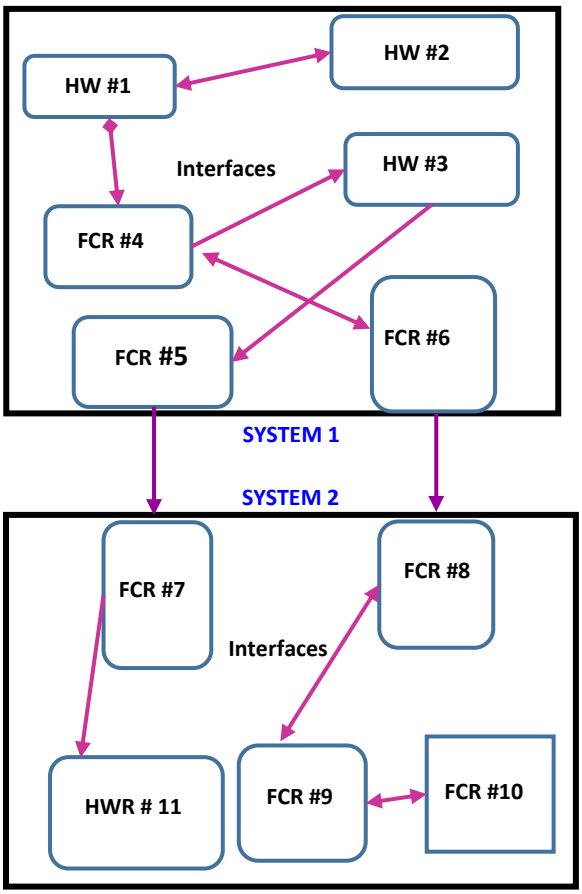

Figure 8. Example of System Solution using EMI FCR

The first main observation from Fig. 8 is that the interfaces between System 1 and System 2 must go through hardware assemblies that are protected with EMI FCRs, as this approach will prevent EMI propagation among systems. In the figure the hardware with EMI FCR#5 in System 1 is connected to the hardware with EMI FCR #7 in System 2. Likewise, the hardware with EMI FCR #6 in System 1 is connected to the hardware with EMI FCR #8 in System 2. The second observation from Fig. 8 is that, within a system, hardware assemblies designed with EMI FCR are placed strategically, which means not every hardware in a system

will need to be designed with EMI FCRs. For example, the hardware containing FCR #4 in System 1 has its internal interface (i.e. within System 1) connected to the hardware with EMI FCR #6 in System 1. This is necessary because these hardware communicate with each other, as shown. However, HWR #3 in System 1, which does not contain an EMI FCR, also communicates with the hardware containing FCR #4, and this is acceptable because communications only flow in one direction (i.e. to the hardware containing EMI FCR #4). We have the same observation in System 2. In System 2, hardware assemblies containing EMI FCRs 8,9, and 10 communicate with each other (i.e. communications flow in mutual directions), hence they must all be protected with EMI FCRs. However, HWR #11 in System 2 does not need an EMI FCR because it receives its communication flow from an EMI FCR hardware (i.e. EMI FCR #7) and HWR #11 does not provide any additional communications paths.

7. Capturing Faults And EMI Propagation In Critical Hardware

Avoiding hardware and software faults and avoiding fault propagation is a constant endeavor in aerospace systems, mostly for safety reasons (i.e. personnel and hardware safety) but also due to the great difficulties often incurred in fault recovery, in a timely manner, or the immeasurable consequences of catastrophic failures. Though to a much lesser extent, EMI propagation is also of concern, because it could induce degraded performance in aerospace hardware and potential faults. In aerospace system fault management software is a prominent line of defense against all types of faults. Fault management software is a subset of flight software and its role is to monitor the health and status of hardware via many of hardware's status indicators. This approach however, addresses only the "symptoms" of a problem. When hardware status indicators show non-compliance, it points to potential existence of problems with the hardware (i.e. "symptoms"), but not necessarily what the problem(s) may be. Fig. 9 proposes a future approach for diagnosis faults caused by EMI propagation and could be adapted for analyzing other types of faults (see Section 3). In the figure HWR #1 with a previously unknown EMI source is connected to HWR #2. EMI is propagated from HWR #1 to HWR #2 because neither one of the hardware has an EMI fault containment region. The proposed solution for diagnosing EMI propagation is a combination of two main elements: (a) an onboard database containing the electrical specs of the signals emanating from the hardware of interest, and (b) an onboard (or ground base) diagnostic tool which in real time compares the electrical specs of the signals coming out from HWR # 1 with the those captured by the diagnostic tool. The comparison tries to find a mismatch in the signal integrity of the HWR # 1 signals. If lack of signal integrity is found then there is strong evidence that EMI propagation has occurred. The same approach can be used in capturing and analyzing faults (see Section 3). In this case of general faults, the database will contain the failure modes of the most common faults for a given hardware and the diagnostic tool compares the actual fault with those in the database. The implementation of these tools are years away from development and would be most useful in high risk manned missions since it requires a large amount of computational resources and the intervention of a crew.

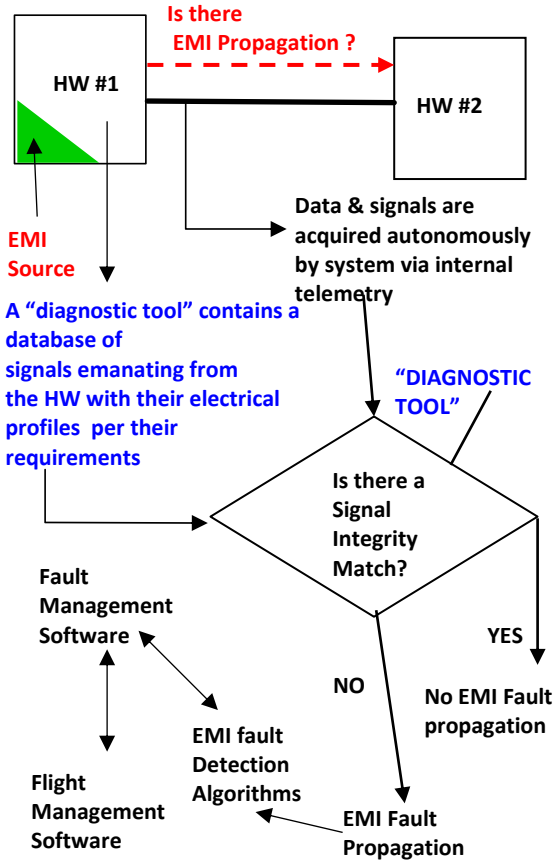

Figure 9. Capturing EMI Propagation in Critical Hardware

9. Summary

The paper introduces the concepts of Fault Containment Regions and EMI Fault Containment Regions, with emphasis on the latter as the main subject of the paper. The paper shows that the knowledge and usage of both types of containment regions can provide significant advantages in the design of aerospace hardware and systems.

Acknowledgement

The work described in this paper was performed under the support of the Jet Propulsion Laboratory of the California Institute of Technology under contract with NASA.

REFERENCES

[1] Lala, J and Harper, R, "Architectural principles for safety critical real time applications," Proc. of the IEEE, ser 1, vol. 82, Jan 1994.

[2] NASA Technical Memorandum 4123, "Evaluation of fault tolerant parallel processor architectures over long Space Missions," National Aeronautics and Space Administration, 1989.

[3] Obermisser, R. "Fault and error containment of gateways in distributed real time systems," Journal of Software, Vol 4, No. 7, Sept. 2009.

[4] NASA Systems Engineering Handbook, SP610S, National Aeronautics and Space Administration, June 1995

[5] Failure Modes Effects and Criticality Analysis, Reliability Analysis Center, Rome Laboratory, Rome, NY, 1993.

[6] Preferred Reliability Practices, Failure Mode effects and Criticality Analysis, PD-AP-1307, National Aeronautics and Space Administration, 2010.

[7] Perez, R, "Integration of analyses in an EMC control plan for avionics hardware in space applications, 2019 IEEE Int. Symposium on EMC, Signal & Power Integrity, July 22-26, New Orleans, LA.

BIOGRAPHIES

Ray Perez, PhD, PE has been employed at the Jet Propulsion Laboratory for 31 years. Ray started as an EMC engineer in his early days but over the years he migrated to design engineering and reliability engineering for electronics designs. He still practices sound EMC principles in design engineering. He has served as the Lead Reliability engineer for many projects.

The research was carried out at the Jet Propulsion Laboratory, California Institute of Technology, under a contract with the National Aeronautics and Space Administration.